Search: ⦿ The ACM Digital Library   ○ The Guide

USPTO

Searching within **The ACM Digital Library** with **Advanced Search**: ("blind signature")   (start a ne
Found **11** of **257,584**

REFINE YOUR SEARCH

▼ Refine by Keywords

Discovered Terms

▼ Refine by People
Names
Institutions
Authors
Reviewers

▼ Refine by
Publications
Publication Year
Publication Names
ACM Publications
All Publications
Publishers

▼ Refine by
Conferences
Sponsors
Events
Proceeding Series

ADVANCED SEARCH
🔍 Advanced Search

FEEDBACK
📝 Please provide us
with feedback

Found **11** of **257,584**

Search Results   Related Journals   Related Magazines   Related S
Related Conferences

Results 1 - 11 of 11   Sort by │relevance   ▾│ in │(

Save results to a Binder

1 Practical multi-candidate election system
Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Gu
August 2001 **PODC '01:** Proceedings of the twentieth annual ACM symposiu
of distributed computing
Publisher: ACM 🖐 Request Permissions

Full text available: 📄 Pdf (898.50 KB)   Additional Information: full citation, abstract, referer
terms

Bibliometrics: Downloads (6 Weeks): 11,   Downloads (12 Months): 53,   Citatior

The aim of electronic voting schemes is to provide a set of protocols tha
cast ballots while a group of authorities collect the votes and output the
paper we describe a practical multi-candidate election scheme that ...

2 Security requirements for internet voting
Rüdiger Grimm
October 2001 **MM&Sec '01:** Proceedings of the 2001 workshop on Multime
new challenges
Publisher: ACM 🖐 Request Permissions
Full text available: 📄 Pdf (481.35 KB) Additional Information: full citation, abstract, referer

Bibliometrics: Downloads (6 Weeks): 3,   Downloads (12 Months): 39,   Citation

In this paper, I describe the security problem of Internet voting system
general security gap of the Internet is described. Second, a possible vot
based on blind signatures is sketched. Third, specific security problems

Keywords: authorization and anonymity, blind signature, internet votir
requirements

**3 Tangler: a censorship-resistant publishing system based on docume
entanglements**
Marc Waldman, David Mazières
November 2001 **CCS '01:** Proceedings of the 8th ACM conference on Compu
Communications Security
Publisher: ACM 🖐 Request Permissions

Full text available: 📄 Pdf (149.02 KB)   Additional Information: full citation, abstract, referer
terms

Bibliometrics: Downloads (6 Weeks): 4,   Downloads (12 Months): 55,   Citation

We describe the design of a censorship-resistant system that employs a document storage mechanism. Newly published documents are depende of previously published documents. We call this dependency an *entangl* Entanglement ...

4 Putting it together: Financial cryptography, the Internet, and the geo
Robert Hettinga
November 1997 **netWorker** , Volume 1 Issue 3

Publisher: ACM   Request Permissions
Full text available: Pdf (842.35 KB)   Additional Information: full citation, index terms

Bibliometrics: Downloads (6 Weeks): 2,   Downloads (12 Months): 17,   Citation

5 Unlinkable serial transactions: protocols and applications
Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **Transactions on Information and System Security (TI**
Issue 4

Publisher: ACM   Request Permissions
Full text available: Pdf (184.87 KB)   Additional Information: full citation, abstract, referer
terms, review

Bibliometrics: Downloads (6 Weeks): 15,   Downloads (12 Months): 81,   Citatior

We present a protocol for unlinkable serial transactions suitable for a va based subscription services. It is the first protocol to use cryptographic subscription services. The protocol prevents the service from tracking ..

Keywords: anoymity, blinding, cryptographic protocols, unlinkable seri

6 Signature schemes based on the strong RSA assumption
Ronald Cramer, Victor Shoup
August 2000 **Transactions on Information and System Security (TISS**
3

Publisher: ACM   Request Permissions
Full text available: Pdf (168.52 KB)   Additional Information: full citation, abstract, referer
terms, review

Bibliometrics: Downloads (6 Weeks): 16,   Downloads (12 Months): 122,   Citatic

We describe and analyze a new digital signature scheme. The new sche efficient, does not require the signer to maintain any state, and can be against adaptive chosen message attack under a reasonable intractabili

Keywords: RSA, digital signatures, provable security

7 Trustee-based tracing extensions to anonymous cash and the makin change
Ernie Brickell, Peter Gemmell, David Kravitz
January 1995 **SODA '95:** Proceedings of the sixth annual ACM-SIAM sympo algorithms
Publisher: Society for Industrial and Applied Mathematics
Full text available: Pdf (1.11 MB)   Additional Information: full citation, references, cited

Bibliometrics: Downloads (6 Weeks): 3,   Downloads (12 Months): 23,   Citation

8 New blind signatures equivalent to factorization (extended abstract)

David Pointcheval, Jacques Stern

April 1997 **CCS '97:** Proceedings of the 4th ACM conference on Computer a
                    communications security

Publisher: ACM Request Permissions

Full text available: Pdf (776.77 KB) Additional Information: full citation, references, cited

Bibliometrics: Downloads (6 Weeks): 4,   Downloads (12 Months): 33,   Citation

9 Strong loss tolerance of electronic coin systems

Birgit Pfitzmann, Michael Waidner

May 1997 **Transactions on Computer Systems (TOCS)** , Volume 15 Issue 2

Publisher: ACM Request Permissions

Full text available: Pdf (267.29 KB) Additional Information: full citation, abstract, referer
                                                                        terms, review

Bibliometrics: Downloads (6 Weeks): 17,   Downloads (12 Months): 78,   Citation

Untraceable electronic cash means prepaid digital payment systems, us
payments, that protect user privacy. Such systems have recently been ¡
considerable attention by both theory and development projects. Howe\
current ...

Keywords: Byzantine faults, electronic cash, payment systems, privac}

10 Meta-ElGamal signature schemes

Patrick Horster, Holger Petersen, Markus Michels

November 1994 **CCS '94:** Proceedings of the 2nd ACM Conference on Comp
                    communications security

Publisher: ACM Request Permissions

Full text available: Pdf (1.16 MB)   Additional Information: full citation, abstract, referer
                                                                        terms

Bibliometrics: Downloads (6 Weeks): 9,   Downloads (12 Months): 71,   Citation

There have been many approaches in the past to generalize the ElGama
scheme. In this paper we integrate all these approaches in a Meta-ElGa
scheme. We also investigate some new types of variations, that haven't
considered ...

11 An efficient fair payment system

Jan Camenisch, Jean-Marc Piveteau, Markus Stadler

January 1996 **CCS '96:** Proceedings of the 3rd ACM conference on Compute
                    communications security

Publisher: ACM Request Permissions

Full text available: Pdf (698.84 KB) Additional Information: full citation, references, cited

Bibliometrics: Downloads (6 Weeks): 8,   Downloads (12 Months): 86,   Citation